Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities

January 2001

IV. Education and Training

IV. Education and Training

Federal Cyber Services (FCS)

Information security/assurance education and training makes good business sense. It provides cost avoidance that could be caused through loss of program productivity, reconstitution of system and data, loss of stakeholder confidence, lower staff morale, and management reaction to additional intrusion attempts. As importantly, the value of due diligence provides program operational survivability, stakeholder confidence, data integrity, higher morale and staff retention.

The *National Plan for Information Systems Protection* announced a new Federal program aimed at addressing the shortage of skilled information assurance/information technology (IA/IT) professionals. The Federal Cyber Services (FCS) training and education initiative is designed to ensure an adequate supply of highly skilled Federal information systems security specialists.

The FCS initiative encompasses five broad programs that will identify IT personnel shortfalls; develop new recruitment, education, and retention efforts; provide continuous training and certification for the many dedicated information security specialists already in government service; and provide information security awareness for all Federal workers. The information systems personnel shortfall is documented by numerous sources, and the nation's reliance on information systems capability is critical to our economic growth.

The FY2001 budget for the FCS civilian program is contained within the National Science Foundation (NSF) and the Office of Personnel Management's (OPM) appropriations. Program planning and coordination within the Federal government is ongoing with the CICG, the CIO Council, the Chief Financial Officers Council, the Human Resource Technology Council, and agencies. Partnership opportunities with industry, non-profit organizations, states, and other professional groups are being initiated.

In addition to the NSF budget request, the National Defense Authorization Act for FY2001 includes a provision authorizing DOD to conduct a program similar to the FCS. This authorization bill includes $20 million for the scholarship program, with a portion of the funds providing financial assistance to build university programs.

OPM Information Technology Occupational Study

One cornerstone of the FCS program, the *OPM IT Occupational Study*, is nearing completion. OPM has issued a Draft Job Family Position Classification Standard for Administrative Work in the Information Technology Group, GS-2200A. (The GS-2200 is a new occupational group for information technology occupations replacing the 0334 occupation series as well as some positions in other series where IT knowledge is paramount.) One of the 11 classification specialty titles in the new guide covers Information Systems Security Specialists, who are estimated at four percent of the current Federal IT workforce. [1] OPM is now conducting a study to validate the competency profiles through a government-wide survey of 22,000 IT employees and supervisors.

[1] Federal IT workforce statistics compiled by OPM: Customer Support positions 14%; Communication and Network services 10%; Data Management 10%; Information Systems Security Specialists 4%, Policy, Planning and

Compilation of agency information gathered by OPM, through close coordination between agencies'[1] IT and human resources staff, shows that Federal IT specialists are an aging workforce. Thirty-five percent of the identified IT workers are over 50 years old, while 52 percent are between 36 and 49. Only 13 percent of the Federal IT workforce is less than 36 years old. With the rapid rate of change within technology, much more attention must be placed on recruitment, retraining, and retaining these workers. OPM estimates show that Federal civilian agencies alone will need to hire 37,000 IT workers over the next six years. The Department of Defense (DOD) employs 43 percent of Federal IT staff, therefore the DOD recruitment need will almost match that of the civilian agencies.

OPM is using the raw data from their study, as well as that developed by the National Security Agency and the National Security Telecommunications and Information Systems Security Committee (NSTISSC) composed of 21 Federal agencies, to develop competency based job profiles for IT personnel including security specialists. The competencies identified for security specialists will become the basis for the Centers for Information Technology (training) Excellence program within FCS. Additionally, OPM has added specific information security competency factors to the competency requirements of all Federal IT positions within the new classification standards.

OPM is using agency ranking and staffing data to review differences in recruitment and retention problems by specialty or work level category (e.g. entry/developmental, full performance, supervisory/managerial position), as well as geographical area. This data will assist OPM in determining additional pay flexibility and/or an IT compensation system to assist agencies to recruit and retain IT employees. As of January 2001 OPM has authorized a special pay rate for IT workers through grade 12. Agencies are currently offering hiring and retention bonuses in order to recruit and retain IT workers.

Scholarship for Service (SFS)

Scholarship for Service, the second of the FCS initiatives, was funded for the first time in FY2001 ($11.2 million). This program will address the shortage of IA/IT professionals by establishing a pipeline for training and recruitment. Specifically, it will provide participants with up to two years of tuition and fees for information security education in exchange for an equal amount of service to the federal government. It will also provide support for faculty and institutional development to increase the number of educational institutions qualified to offer SFS opportunities. The NSF and the OPM are jointly administering SFS. The review of university grant proposals is in progress, with university awards to be announced in spring 2001. The first cohort of SFS students will begin studies in fall 2001.

NSF has developed and coordinated with the CICG the application requirements and project design for the SFS grant program. The NSF Board of Directors approved the SFS program and management plans, and the program announcement is completed. Three tracks are included in the SFS program announcement: student scholarships, faculty development and facility development. Collectively these tracks will assist the development of a strong cyber security program at numerous colleges and universities.

Management 10%; Software Engineering Applications 18%; Software Engineering Systems 6%; Systems Administrators 10%; Systems Analysts 9%; Web Developers 2%; General 5%; unclassified 2%.

[1] OPM received reports from 38 agencies plus the President's Council on Integrity and Efficiency, representing agency Office of Inspect General. Approximately 90% of the actual Federal IT workforce is included in the reports.

The SFS start-up funding in the FY2001 budget provides two-year scholarships for up to 100 M.S. candidates or two-year scholarships for promising juniors and seniors working towards a B.S. in an accredited information security program. The target for the program is to produce 300 bachelors and/or masters' degree graduates annually with an emphasis in information security. Other benefits to the program will be outreach to under-represented and economically disadvantaged students, an increase in the information security expertise in academia, support for continuing education, and support for R&D at universities.

University outreach will be conducted through NSF's normal grant proposal process, direct contact with the fourteen universities recognized by NSA as Centers of Excellence in Information Assurance Education, direct contact with the participants in the FY2000 National Colloquium for Information Systems Security Education (Colloquium), and direct contact with all other schools who have inquired to NSF about the grant program to date.

Center of IT (Training) Excellence (CITE)

The third program within the FCS initiative is the *Center of IT (Training) Excellence* (CITE) for information security skills. The CITE will provide high-caliber, cutting-edge information security training and certification for current Federal IT security employees, Federal contractors, and FCS candidates. The CITE is conceived as a virtual, nationwide network of "recognized" public and private training centers that meet information security competencies defined by OPM and based on OPM, NSF, NSTISSC, CIO Council, industry, and other requirements. These competencies will be part of OPM's IT Occupational Survey, to be completed spring 2001, and will be used as the basis for development of the competency requirements for security positions. Initial development of the CITE will focus on providing training for Systems Administrators and Information Systems Security Officers (ISSOs).

A proposed project plan for the CITE program was developed. Multiple forms of training delivery are included in order to provide high-caliber, cutting-edge information security training any time, any place, to maintain technical skills within Agencies current with the state-of-the-art technology development, and to provide growth for current Federal information security professionals.

Identified in the *National Plan*, the issue of employee certification has not been resolved at this time. Employee certification is actively encouraged at Federal agencies, some of which are paying bonuses to workers with such official skills recognition. A Federal-wide policy mandating certification of workers has not been adopted. However, four universities are experimenting with inclusion of the SANS education/certification programs as part of their undergraduate and graduate programs in FY2001. SANS education/certification programs require both testing and practical work.

High School and Secondary School Awareness and Outreach Program

The fourth program in the FCS initiative, the *High School and Secondary School Awareness and Outreach Program*, has a large, future payback for the nation. Outreach to high schools and secondary schools will ultimately expand information security awareness into homes and communities. Numerous programs have begun to address this issue, with industry taking the lead. Programs are being developed to increase awareness of the vulnerability of information systems and institute a cyber ethics curriculum for high school and secondary schools. In order for these programs to be successful, they provide teaching standards in computer security practices and ethics.

The National Academy Foundation (NAF)[1] launched a new Academy of Information Technology (AoIT). The program will prepare high school students for careers in IT fields. AoIT will provide ninth through twelfth grade curriculum, with opportunities to partner with community colleges, universities, and businesses. Twelve pilot sites were chosen for implementation in fall 2000, to reach a total of 350 to 400 students. In fall 2001, 40 new schools will be added, with an increase of 40 to 50 per year depending on full industry support.

The Department of Justice, through the Information Technology Association of America, initiated the Cyber Citizen program to raise security awareness and teach cyber ethics. Also, the Defense Information Systems Agency (DISA) has met with many agencies and non-profit organizations offering their security awareness materials, especially the Cyber Protect "game" they developed to simulate practical application of security techniques. The Department of Commerce is partnering in a national media campaign to promote a positive image of technical jobs. This campaign was launched this fall in connection with the second annual National Techies Day on October 3.

Federal Information Assurance Awareness Campaign

The fifth program in the FCS initiative, the *Federal Information Assurance Awareness Campaign*, is designed to ensure that all IT systems users are aware of security threats, their personal responsibilities to deter threats, and the security practices that will help safeguard critical information. The CIO Council conducted a Critical Infrastructure Protection (CIP) Day to foster increased emphasis on CIP. In addition, the CIO Council determined that most agencies need updated training materials. Activities have focused on sharing materials or, in some cases customizing quality programs from DISA. The Federal Information Systems Security Educators Association (FISSEA) and the Federal Computer Security Program Managers Forum are sharing information about agency programs in order to assist this process.

Finally, the Office of Science and Technology Policy is researching the shortage in the number of academic professionals who are teaching and performing basic research in information security. The purpose of their report is to "increase the number of people both graduating with advanced degrees and teaching and performing basic research in the field of information security/assurance and critical infrastructure protection (ISA/CIP)."[2] Suggested findings are that "there are not enough ISA/CIP experts currently teaching and performing basic research to meet the current demand; there are not enough Doctoral students currently specializing in IS to meet future demand; short-term applied research is being emphasized over long-term basic research; and industry-efforts alone will not solve these problems."[3] When this research is completed, the OSTP will publish a full report with recommendations to alleviate the problem.

[1] President Clinton and Sanford I. Weill, Chairman of Citigroup and the National Academy Foundation, announced the program on July 6, 1999.
[2] OSTP draft Academic Initiative Proposal, revised September 5, 2000, in review at this time.
[3] Ibid.